



# United States Department of the Interior


OFFICE OF THE SECRETARY  
Washington, DC 20240



OCIO Directive 2006-010

MAR 20 2006

To: Assistant Secretaries  
Heads of Bureaus and Offices

From: W. Hord Tipton   
Chief Information Officer

Subject: Instant Messaging, Internet Relay Chat, Web Conferencing, and Peer-to-Peer Usage Policy

## Purpose and Scope

This directive issues Instant Messaging (IM), Internet Relay Chat (IRC), Web Conferencing and Peer-to-Peer (P2P) usage policy for all users of information systems, Government- and contractor-managed, in all DOI bureaus, offices, and contractor facilities where such information systems exist.

## Policy

1. DOI OCIO Technical Bulletin No. 2003-nnn, "Peer-to-Peer" file sharing restriction, issued July 28, 2003, is hereby rescinded.
2. Unauthorized use, installation, or activation of IM, IRC, web conferencing, and P2P is prohibited.

## All Information Systems

3. Authorized use, installation, or activation of IM, IRC, web conferencing, and P2P shall only be granted by the information system's Designated Approving Authority (DAA), *other than expressly authorized in §5*.
  - a. Authorization requests shall be submitted to and approved by the respective DAA prior to any use.
    - i. Authorization artifacts shall be recorded in the System Security Plan (SSP) and Risk Assessment (RA).
  - b. Authorization requests shall also be submitted to and approved by the DAAs of all associated interconnected systems, where said application and service traffic traverses the interconnection boundary, prior to any use.
    - i. Authorizations shall be recorded in the appropriate interconnection security agreements.

- ii. Authorization artifacts shall also be recorded in the SSP and RA of all associated interconnected systems.
  - c. The SSPs and RAs shall collectively:
    - i. Describe all security controls required for authorization;
    - ii. Identify the risks to the information and information system(s); and
    - iii. Include the DAA's authorization(s) and statements acknowledging and accepting the risks.
  - d. The DAA level of authorization does not require comprehensive user lists, deferred to §4c(ii), only a general user list (e.g., roles, divisions).
4. Authorized use, installation, or activation of IM, IRC, web conferencing, and P2P shall comply with the following provisions. *other than expressly authorized in §5:*
- a. Users shall be authenticated against a DOI trusted user list (e.g., Active Directory)
  - b. Use is restricted to intranets, i.e., closed DOI environments, except as specifically noted below:
    - i. Public Internet use is permitted only by authorized users meeting the following qualifications, *while not violating a Court Order*:
      - 1. Working with or having recognized disabilities needing this technology (speech, hearing, or sight); or
      - 2. Conducting necessary official business where no other forms of communication are sufficient and only when all other provisions are met.
    - ii. Furthermore, any transmission of Sensitive but Unclassified (For Official Use Only) information over the public Internet shall use authorized end-to-end encryption algorithms (FIPS 140-x, most current revision).
  - c. Bureaus and offices shall:
    - i. Standardize on IM, IRC, web conferencing, and P2P applications and services based on approved technology in the Technical Reference Model.
    - ii. Account for all authorized users.
    - iii. Implement technical controls to restrict use to only authorized users.
    - iv. Implement appropriate management, operational, and technical controls to ensure appropriate capture and retention of:
      - 1. Federal records as defined in 44 U.S.C. 3301; and specifically
      - 2. electronic communications that relate to the:
        - a. American Indian trust reform, including High-Level Implementation Plan or any of its subprojects;

- b. Cobell v. Norton litigation; or
- c. Administration of Individual Indian Money accounts.
- v. Implement capabilities within their configuration management process to detect and remove unauthorized IM, IRC, web conferencing, and P2P software.

Bureaus and offices and the ESN shall:

- vi. Implement technical controls to prevent IM file attachments from traversing across their managed Internet gateways.
  - vii. Apply technical controls that provide a fail-safe mechanism to disable IM through all Internet gateways within 30 minutes of an order from the Departmental Chief Information Officer.
  - viii. Notify affected bureaus and offices of IM threats that require activation of IM disabling controls.
5. Emergency authorizations and exceptions to the provisions, as defined in §3-4, of IM, IRC, web conferencing, and P2P use may be granted by the Departmental Chief Information Officer, when found necessary to prepare for or address situations where other means of communication are not sufficient or may be unreliable. Only the Departmental CIO may delegate emergency authorization or waivers.
6. Initial compliance action:
- a. All information systems shall be fully inspected, to detect unauthorized software, by June 1, 2006.
  - b. All unauthorized software shall be fully removed by August 1, 2006.

References

1. Information Bulletin: Unauthorized Peer to Peer (P2P) Programs on Government Computers. April 19, 2005. Department of Homeland Security.
2. Memorandum: M-04-26 Personal Use Policies and "File Sharing" Technology. September 8, 2004, Office of Management and Budget.

Definitions

1. Instant Messaging (IM) – a form of electronic communication (text-based) which involves immediate correspondence (usually through a messaging service) between two or more users who are all online simultaneously. Popular messaging services include AOL (Instant Messenger), Yahoo, and MSN.

2. Internet Relay Chat (IRC) – a form of electronic communication (text-based) over a large network of chat channels (chat rooms, party-line, conference system) that allows users to correspond simultaneously. Popular IRC networks include Undernet, Galaxynet, and ERNet.
3. Web Conferencing – a technology which delivers electronic communication and collaboration (screen sharing, white board, video feeds) via Internet channels by service providers. Popular web conferencing applications include WebEx, Live Meeting, QuickPlace, WebSphere Portal, and Sametime.
4. Peer-to-Peer (P2P) – an application and network connection that allows a group of computer users to connect with each other for the purposes of directly accessing files from one another's computers. Popular P2P applications and services include: Kazaa, Morpheus, and Warez.

*Contact the Cyber Security Division for a complete list of known applications and commonly used network ports.*

### **Contact Information**

If you have any questions or comments regarding this directive, you may contact my office at (202) 208-6194. Staff may contact Mr. Larry Ruffin, Acting Chief, Cyber Security Division at (202) 208-6425 or (202) 208-5419.